플로우의 연관성 모델과 시드 기반의 연속적인 그룹핑을 이용한 악성 트래픽 탐지

박지태, 이성호, 구영훈, Huru Hasanova, 김명섭
고려대학교
{pjj5846, gaek5, gyh0808, hhuru, tmskim}@korea.ac.kr

Attack Traffic Detection using the Correlation of the Flow and Seed based Sequential Grouping Model

Jee-Tae Park, Sung-Ho Lee, Young-Hoon Goo, Huru Hasanova, Myung-Sup Kim
Korea Univ.

요 약

오늘날의 네트워크는 인터넷 환경의 고속화와 과학 기술의 비약적인 발전으로 인해 점점 복잡해지고 다양해지고 있다. 이에 Malspam, Ransomware 등 악성 트래픽의 종류와 패턴도 같이 복잡해지고 있는 추세이다. 이러한 추세에 대응하기 위해서는 악성 트래픽에 대하여 정확한 탐지 및 분석이 필요하고, 이에 현재 많은 연구가 진행되고 있다. 기존의 가장 보편적으로 알려진 방법은 페이로드 시그니처 기반의 탐지 기법과 기계학습을 이용한 방법이다. 페이로드 시그니처 기반의 방법은 높은 정확도와 분석률을 지니지만 사용하기 불편하고 번거롭다는 단점이 있다. 기계학습 기반의 방법은 역시 편리하고 높은 정확도 및 분석률을 지니지만 충분한 양질의 데이터가 반드시 필요하다는 단점이 있다. 이에 본 논문에서는 시드 기반의 연속적 그룹핑 모델을 이용한 악성 트래픽 탐지 시스템을 제안한다. 제안한 탐지 시스템을 실제 악성 트래픽에 적용하여 실험을 진행했을 때, 높은 정확도와 분석률의 결과를 얻을 수 있었다.

Ⅰ. 서 론

오늘날 네트워크는 인터넷 환경의 고속화와 과학 기술의 비약적인 발전으로 인해 급속도로 성장하고 있다. 날이 갈수록 복잡해지는 네트워크 환경의 추세에 따라 악성 트래픽의 종류와 패턴도 복잡해지고 있고, 악성 트래픽에 의한 피해도 점점 커지고 있다. 이를 방지하기 위해서는 악성 트래픽을 정확하게 탐지하고 분석해야 한다. 현재 까지 많은 연구가 진행되어 왔고, 여러 방법들 중 가장 보편적인 탐지 기법은 페이로드 시그니처와 기계학습을 이용한 방법이다[1,2].

페이로드 시그니처를 이용한 탐지 방법은 헤더 등의 시그니처를 이용하여 분류하는 방법이며, 정확도와 분석률 측면에서 가장 높은 성능을 지닌다[2]. 하지만 미리 정의된 트래픽 시그니처의 패턴에 너무 의존적이며, 시그니처 추출 작업이 수작업으로 진행되기 때문에 실시간으로 다양한 트래픽을 처리해야 하는 네트워크에서는 적합하지 않다[1]. 즉 이러한 페이로드 시그니처를 이용한 탐지 방법은 새로운 트래픽이 발생했을 때 대처하기 힘들고 적용하기에 너무 복잡하다는 단점을 가지고 있다. 기계 학습을 이용한 탐지 방법은 트래픽의 특징을 학습하여 이를 바탕으로 탐지하는 방법이다. 이 방법은 페이로드 시그니처 기반의 탐지 방법보다 적용하기 쉽고 편리하다는 점에서 장점을 가지고 있다. 하지만 높은 정확도와 분석률을 지니기 위해서는 많은 양의 샘플 데이터의 확보가 필수적이다[1]. 즉, 학습 데이터에 따라서 결과가 크게 달라지므로 상황에 따라서 적합 하지 않을 수 있다.

따라서 본 논문에서는 네트워크 플로우의 연관성 모델과 시드 기반의 순차적인 그룹핑을 이용한 악성 트래픽 탐지 방법을 제안한다. 이 후 제안하는 방법을 바탕으로 실제 악성 트래픽을 이용하여 실험 한 후 정확하게 탐지 되는지 확인한다.

본 논문의 구성은 본 장의 서론에 이어 2장 본론에서 제안하는 탐지 방법과 시스템에 대하여 설명한다. 다음 3장에서 실제 악성 트래픽을 적용한 실험을 진행 하여 그 결과를 확인한다. 마지막으로 4장에서는 결론 및 향후 연구에 대해 언급한 뒤 본 논문을 마친다.

Ⅱ. 본론

본 논문에서는 제안하는 악성 트래픽 탐지 시스템은 총 4 가지의 모듈로 구성되어 있으며, 전체적인 구조는 그림 1과 같다.

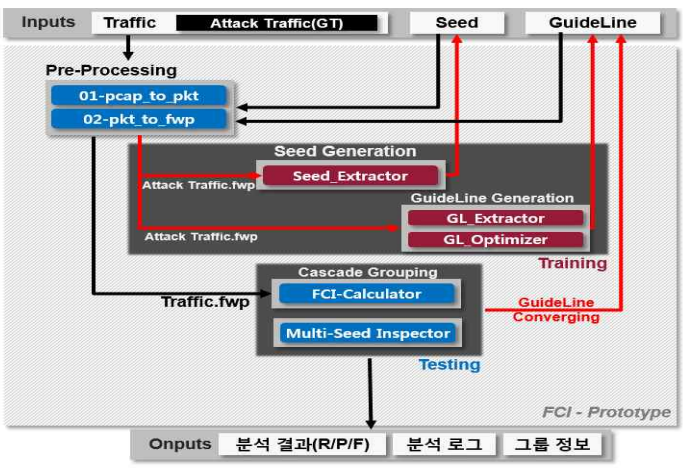

그림 1. 연속적 그룹핑을 통한 악성 트래픽 탐지 시스템 구조

먼저 Input으로는 악성 트래픽과 노이즈 트래픽 (비악성 트래픽)이 섞여있는 트래픽, 시드, 가이드라인이 있고, Output 으로는 분석 결과와 분석로그, 그룹핑된 정보가 있다. 시드와 가이드라인은 각각 Seed

이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단 기초연구사업과 (No.2015R1D1A3A01018057) 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No. 2017-0-00513, Security Analytics 기반의 이기종 보안솔루션 위협 분석 및 대응 기술 개발)

Generation과 Guideline Generation 모듈에서 중간 결과로 나온다. 최종적으로 악성 트래픽 탐지는 마지막 모듈인 Cascade Grouping에서 트래픽, 시드, 가이드라인을 이용하여 탐지한다. 각 모듈에 대한 상세 설명은 다음과 같다.

첫 번째 모듈은 Pre-Processing 이고, 이 모듈은 Input으로 들어온 트래픽 (pcap)을 fwp로 바꿔주는 역할을 한다. 두 번째 모듈은 Seed Generation 이고, 이 모듈은 Pre-Processing된 트래픽의 5-tuples 정보를 모아서 텍스트 파일로 저장하고 이를 시드라고 정의 한다.

세 번째 모듈에서는 Guideline Generation 이고, 이 모듈에서는 Guideline Extractor과 Guideline Optimizer로 구성되어 있고 전반적인 구조는 그림 2와 같다.

먼저 가이드라인은 그룹핑을 위한 유사성, 연결성의 인덱스 기준값 (Threshold)과 가중치(Weights)를 정의한다. 유사성 인덱스는 Source Flow와 Target Flow의 유사성을 이용하여 계산하는 값이다. 이는 Flow Size와 Inter Arrival Time에 대한 정보를 가지고 Euclidean Distance의 공식을 이용하여 계산한다[1]. 그리고 연결성 인덱스의 값은 Source Flow와 Target Flow의 순차적인 연결성을 이용하여 계산하는 값이다. 이는 Flow의 5-tuple 정보를 비교하여 각각의 가중치를 곱하여 계산한다[1].

Guideline Extractor에서는 각 시드별로 위의 유사성 및 연결성 인덱스 및 가중치의 값들이 나온다. 후에 Guideline Optimizer에서 Guideline Extractor에서 추출된 가이드라인을 Threshold Optimization통하여 최적화 시킨다.

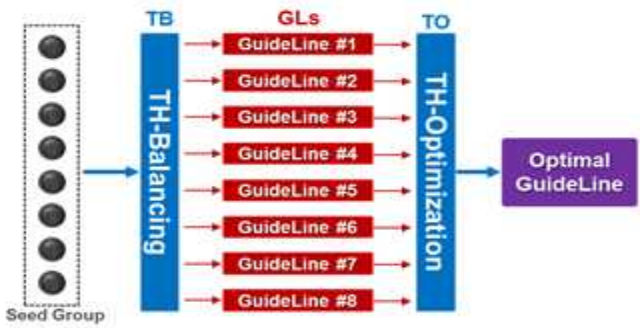

그림 2. Guideline Generation 모듈의 전반적인 구조

네 번째 모듈에서는 Cascade Grouping 이고, 이 모듈에서는 이전 모듈의 가이드라인과 트래픽을 가지고 순차적으로 그룹핑을 하는 단계이다. Cascade Grouping 모듈의 구조는 그림 3와 같다.

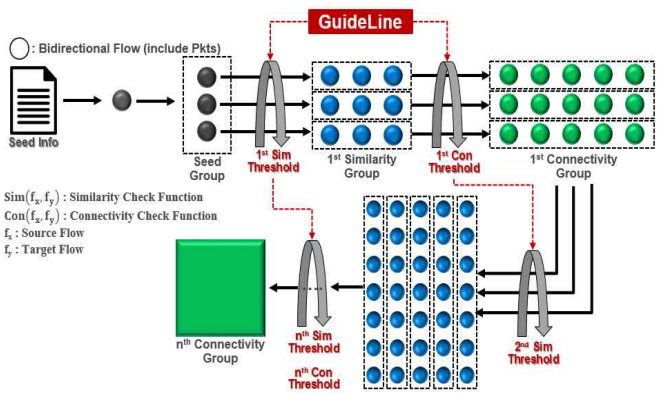

그림 3. Cascade Grouping 모듈의 전반적인 구조

먼저 이전 모듈에서 생성된 시드를 가지고 시드 그룹을 만든다. 시드 그룹은 확실하게 악성으로 탐지된 트래픽의 시드를 기반으로 만든 그룹이다. 시드 그룹과 가이드라인을 가지고 유사성과 연결성 그룹으로 순차적으로 그룹핑을 진행한다. 그룹핑이 진행됨에 따라 탐지되는 악성 트래픽은 점차적으로 늘어나게 되고, 더 이상 그룹핑이 되지 않을 때 까지 진행한다. 마지막으로 그룹핑이 된 트래픽이 최종적으로 탐지된 악성 트래픽이고 이에 대해 정확도와 분석률이 결과로 나온다.

Ⅲ. 실험

본 논문에서 제안한 시스템의 타당성을 검증하기 위하여 실제 악성 트래픽과 노이즈 트래픽을 적용하여 실험을 진행하였다.

ATTACK TRAFFIC				
Trace #	Attack Type	Size		
		Flow	Pkt	Byte
1	MalSpam	71	18,055	15,167,725
2	GodZilla-Loader	69	1,862	1,358,410
NOISE TRAFFIC				
Trace #	Application Type	Size		
		Flow	Pkt	Byte
1	Chrome, IE web	491	60,266	46,852,995
2	Skype	576	107,534	95,635,596

표 1. 실험에 사용한 악성 및 노이즈 트래픽 정보

우선 실험에 사용한 노이즈 트래픽은 Skype, Chrme 등의 웹 브라우저 및 메신저 응용 트래픽을 사용하였고, 악성 트래픽은 Malspam, GodZilla-Loader를 사용하였다. 실험에 사용한 트래픽의 상세 정보는 표 1과 같다. 실험은 악성 트래픽의 종류에 따라 총 두 가지로 나누어 진행하였고, 사용한 노이즈 트래픽은 각각의 Trace 에 따라 나누어 사용하였다.

Detection Result						
Trace #	Attack Type	Noise Traffic	Measurement	Coverage (%)		
				Flow	Pkt	Byte
1	MalSpam	all	Recall	100	100	100
			Precision	100	100	100
2	GodZilla-Loader	all	Recall	96.4	97.5	98.8
			Precision	100	100	100

표 2. 악성 트래픽 탐지 실험 결과

제안한 시스템을 이용하여 악성 트래픽 탐지 실험한 결과는 표 2와 같다. 먼저 Trace 1의 Malspam의 경우에는 Flow, Pkt, Byte에서 모두 Recall과 Precision이 100%의 결과가 나타났다. 다음으로 Trace 2의 GodZilla-Loader 의 경우 Precision에서는 모두 100%가 나왔지만 Recall 측면에서는 Trace 1보다 조금 낮은 96 - 99%의 결과가 나타났다.

Ⅳ. 결론 및 향후 연구

본 논문은 플로우의 연관성 모델과 시드기반의 연속적 그룹핑을 적용하여 악성 트래픽 탐지하는 시스템을 제안하였고, 실제 악성 트래픽을 적용한 실험을 통해 검증하였다. 특히 실험에서 높은 정확도와 분석률을 통하여 그 타당성을 입증하였다. 따라서 향후 연구로는 더욱 다양한 종류의 악성 트래픽을 적용하여 실험을 진행할 계획이다.

참 고 문 헌

[1] 구영훈, 심규석, 이성호, Baraka D. Sija, and 김명섭 " 네트워크 플로우의 연관성 모델을 이용한 트래픽 분류 방법" 정보과학회 논문지. Vol.44 No.04 April. 2017. pp433-438

[2] 박준상, 윤성호, 안현민, 김명섭, "페이로드 시그니쳐 기반 인터넷 트래픽 분류" , May, 15-16, 2014, pp10-14